PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-049591

(43)Date of publication of application : 15.02.2002

(51)Int.Cl. G06F 15/00
H04L 9/32
H04M 11/00

(21)Application number : 2001-145172

(22)Date of filing : 15.05.2001

(71)Applicant : MARUJU SHOKAI:KK

(72)Inventor : MATAYOSHI MORIO

(30)Priority

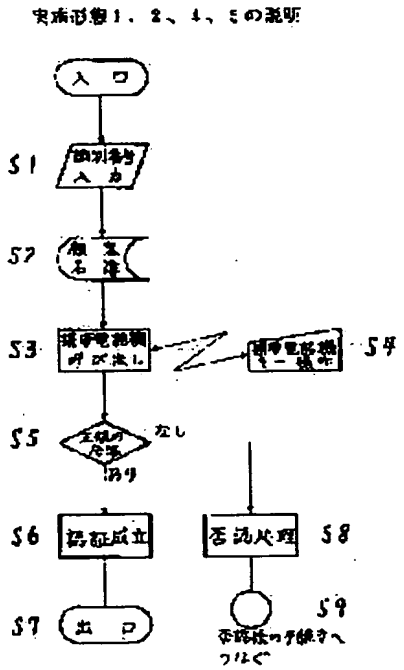
Priority number : 2000141470 Priority date : 15.05.2000 Priority country : JP

(54) SYSTEM AND METHOD FOR PERSONAL AUTHENTICATION

(57)Abstract:

PROBLEM TO BE SOLVED: To discriminate genuineness of a user with higher assurance by using a method other than the conventional password numbers or changing the using method of password numbers about a user genuineness discrimination method (personal authentication method) that uses a computer when a cash card, the electronic commerce, the Internet, a burglar preventing system, etc., are used.

SOLUTION: In this user genuineness discrimination method, the preliminarily registered cellular phone number of a user is retrieved from a storage by means of the user identification information (customer number, user name, etc.), when this user identification information is inputted from an information terminal (external device). Then the user's cellular phone is called via a communication means and the user's identity is recognized when a specific input operation is carried out via the cellular phone.



LEGAL STATUS

[Date of request for examination] 15.05.2002

[Date of sending the examiner's decision of rejection] 29.06.2004

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision 2004-15685

of rejection]

[Date of requesting appeal against examiner's decision of rejection] 28.07.2004

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開2002－49591
（P2002－49591A）
(43)公開日　平成14年２月15日(2002.2.15)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　15/00	３３０	Ｇ０６Ｆ　15/00	３３０Ｂ	５Ｂ０８５
Ｈ０４Ｌ　9/32		Ｈ０４Ｍ　11/00	３０２	５Ｊ１０４
Ｈ０４Ｍ　11/00	３０２	Ｈ０４Ｌ　9/00	６７３Ｅ	５Ｋ１０１

審査請求　未請求　請求項の数８　ＯＬ　（全 10 頁）

(21)出願番号　特願2001－145172(P2001－145172)
(22)出願日　平成13年５月15日(2001.5.15)
(31)優先権主張番号　特願2000－141470(P2000－141470)
(32)優先日　平成12年５月15日(2000.5.15)
(33)優先権主張国　日本（ＪＰ）

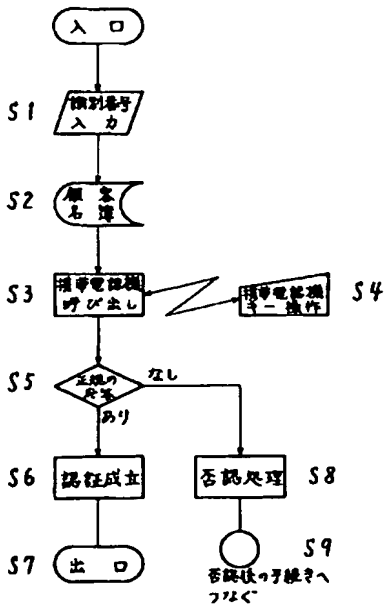
(71)出願人　500218611
合資会社　丸十商会
沖縄県那覇市牧志３丁目13番17号　丸十ビル内
(72)発明者　又吉　盛雄
沖縄県那覇市牧志３丁目13番17号　丸十ビル内
(74)代理人　100076082
弁理士　福島　康文

Ｆターム(参考)　5B085 AE02 AE04 AE23
5J104 AA08 KA01 NA05 PA02
5K101 LL12 NN02 PP04

(54)【発明の名称】　個人認証システムおよび個人認証方法

(57)【要約】
【課題】キャッシュカードや電子商取引、インターネット、防犯システム等を利用する際における、コンピュータを利用した利用者の真偽鑑別方法（個人認証方法）に関し、従来の暗証番号以外の方法、もしくは、暗証番号の使用方法を変えることで、より確実に利用者の真偽鑑別を可能とする。
【解決手段】利用者の識別情報（顧客番号、利用者名など）が情報端末（外部装置）より入力されたとき、あらかじめ登録されているその利用者の携帯電話番号を、利用者識別情報（顧客番号、利用者名など）をもとに記憶装置より検索し、その利用者の携帯電話機を通信手段を介して呼び出し、該携帯電話機より特定の入力操作がなされたときに、その利用者本人であると認定することを特徴とする利用者の真偽鑑別方法である。

実施形態１、２、４、５の説明



1

【特許請求の範囲】

【請求項１】　個人の識別情報（顧客番号、利用者名、住民番号など）を入力するための識別情報入力手段、
個人の識別情報および携帯電話番号をあらかじめ登録（記憶）しておく記憶手段、
識別情報入力手段より入力された個人の識別情報をもとに該記憶手段より検索し読み出したその個人の携帯電話番号の携帯電話機を呼び出す通信手段、
個人が所有（所持）する応答操作のための携帯電話機、
該携帯電話機より通信手段を介して送られた応答信号を正規な応答であるか判断する演算手段を有しており、
この演算手段の判断に基づき、その個人を本人であると認証する構成になっていることを特徴とする個人認証システム。

【請求項２】　個人の識別情報（顧客番号、利用者名、住民番号など）が識別情報入力手段（情報端末）より入力されたとき、あらかじめ記憶手段に登録されているその個人の携帯電話番号を、個人の識別情報をもとに該記憶手段より検索して、その個人の携帯電話機を通信手段を介して呼び出し、該携帯電話機より特定の入力操作（応答操作）がなされたときに、その信号（応答信号）を受信して正規な入力操作がなされたかを判断し、その個人本人であると認定することを特徴とする、個人認証方法。

【請求項３】　個人の識別情報（顧客番号、利用者名、住民番号など）および携帯電話番号が記録された個人カード（キャッシュカード、クレジットカード、メンバーズカード、行政ＩＣカード等）、
該個人カードを使用して個人の識別情報および携帯電話番号を入力するための識別情報入力手段、
該識別情報入力手段より読み出した携帯電話番号の携帯電話機を呼び出す通信手段、
個人が所有（所持）する応答操作のための携帯電話機、
該携帯電話機より通信手段を介して送られた応答信号を正規な応答であるか判断する演算手段を有しており、
この演算手段の判断に基づき、その個人を本人であると認証する構成になっていることを特徴とする個人認証システム。

【請求項４】　個人の識別情報と携帯電話番号が記録されている個人カード（キャッシュカード、クレジットカード、メンバーズカード、行政ＩＣカード等）を使用して、個人の識別情報と携帯電話番号が識別情報入力手段より入力されると、その個人が所有する携帯電話機を通信手段を介して呼び出し、該携帯電話機から特定の入力操作（応答操作）がなされたとき、その信号（応答信号）を受信して適正な応答操作がなされたかを判断し、その個人本人であると認定することを特徴とする個人認証方法。

【請求項５】通信手段を介して互いに接続された複数のコンピュータ間において、運営者側のコンピュータが、

2

利用者側コンピュータの利用者個人を確認するための利用者の個人認証システムであり、
利用者は利用者側コンピュータに利用者（個人）の識別情報入力手段を持ち、さらに応答操作のための携帯電話機を持ち、
運営者側のコンピュータは、あらかじめ利用者の識別情報と、携帯電話番号を記憶手段に登録しておき、利用者側コンピュータの識別情報入力手段より入力された個人の識別情報をもとに該記憶手段より検索して読み出した携帯電話番号の携帯電話機を呼び出す通信手段、
該携帯電話機より通信手段を介して送られた応答信号を正規な応答であるか判断する演算手段を有しており、
この演算手段の判断に基づき、その利用者本人であると認定する構成となっていることを特徴とする個人認証システム。

【請求項６】　通信手段を介して互いに接続された複数のコンピュータ間において、利用者側のコンピュータから利用者の識別情報が入力され送信されたとき、これを受信し、運営者側のコンピュータ（相手を利用者認定するべき側のコンピュータ）において、あらかじめ登録されたその利用者の携帯電話番号を、利用者の識別情報をもとに記憶手段より検索して、その利用者の携帯電話機を通信手段を介して呼び出し、該携帯電話機より特定の入力操作（応答操作）がなされたとき、その信号を受信して適正な入力操作（応答操作）がなされたかを判断し、その利用者本人であると認定することを特徴とする利用者の個人認証方法。

【請求項７】　前述の携帯電話機に代えて、双方向通信手段を用いることを特徴とする請求項１から請求項６までのいずれかに記載の個人認証システムまたは個人認証方法。

【請求項８】　該携帯電話機より入力される特定の入力操作（応答操作）が暗証番号であることを特徴とする請求項１から請求項７までのいずれかに記載の個人認証システムまたは個人認証方法。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、キャッシュカードや電子商取引、インターネット、防犯システム等を利用する際における、コンピュータおよび通信手段を利用した個人認証システム、および個人認証方法に関する。

【０００２】

【従来の技術】近年コンピュータや通信手段の発達により、キャッシュカードやデビットカードに見られるように、暗証番号を入力するだけでその利用者本人であると認識して、出金や決済が可能となって来ている。

【０００３】また、インターネットなどを介して暗証番号（パスワード）を入力することで、不特定多数の利用者が遠隔地から他のコンピュータを利用できるなど、大変便利になってきた。

【０００４】
【発明が解決しようとする課題】しかし、本来、暗証番号は他人に見られたり、解読される可能性も決してないとはいえず、不正使用されないか、不安が残るものである。
【０００５】また、インターネット上での利用者の識別に関しても、暗証番号（パスワード）を解読するといった、不正な利用者のプログラムによって不正侵入される事件が後を絶たない。
【０００６】したがって、このような暗証番号による完璧な利用者の個人認証システムおよび方法は、現在ほとんど皆無である。
【０００７】本発明の技術的課題は、このような問題に着目し、従来の暗証番号以外の方法、もしくは、暗証番号の使用方法を変えることで、より確実に個人認証および利用者の識別を可能とすることにある。
【０００８】
【課題を解決するための手段】本発明の技術的課題は、次のような手段によって解決される。請求項１は携帯電話機等の移動通信手段と該携帯電話機を呼び出すための通信手段およびコンピュータを利用した個人認証システムであり、以下の各手段を有している。
１．個人の識別情報（顧客番号、利用者名、住民番号など）を入力するための識別情報入力手段。これは、入力キーもしくはカードリーダー等の情報端末による。銀行が使用するキャッシュディスペンサーや、デビットカードを使用する際のカードリーダー等がこれに相当する。
２．個人の識別情報および携帯電話番号をあらかじめ記憶しておく記憶手段。これは前述の識別情報入力手段等の情報端末装置内部に置いても良いが、情報処理センターや電子認証センターのコンピュータシステム内に置くのが望ましい。
３．識別情報入力手段より入力された個人の識別情報をもとに記憶手段より検索し読み出した携帯電話番号の携帯電話機を呼び出す通信手段。
４．個人が所有（所持）する応答操作のための携帯電話機。
５．携帯電話機より通信手段を介して送られた応答信号を正規な応答であるか判断する演算手段。
【０００９】以上の各手段を有するシステム構成により、演算手段の判断に基づき、その個人を本人であると認証する。なお、本システムに使用する携帯電話機は、通常の携帯電話機を使用でき、携帯電話機に特別な付加機能などを設ける必要はない。
【００１０】請求項２は携帯電話機等の移動通信手段と該携帯電話機を呼び出すための通信手段およびコンピュータを利用した個人認証方法であり、例えば顧客番号や利用者名、住民番号（個人番号）などのような、個人の識別情報が、識別情報入力手段（情報端末）からのキーによる操作あるいは個人カード等を利用して入力されたとき、あらかじめその識別情報入力手段（情報端末装置）の内部あるいは情報処理センター、もしくは電子認証センターのコンピュータの記憶装置に登録されているその利用者の携帯電話番号を、利用者個人の識別情報をもとに記憶装置より検索して、通信手段を介してその番号の携帯電話機を呼び出し、携帯電話機から携帯電話機の所有者すなわち本人による特定の入力操作（応答操作）がなされたとき、その利用者本人であることを認定する。呼び出し後、ある一定時間内にその特定の入力操作（応答操作）がなされないときは、否認する。以上の個人認証方法である。
【００１１】前記の個人カード等には、キャッシュカード、クレジットカード、メンバーズカードあるいは、現在政府が策定中の行政ＩＣカード等が含まれるものとする。
【００１２】このとき、携帯電話機の所有者による特定の入力操作すなわち応答操作とは、携帯電話機の応答保留ボタンを１回押して応答保留にするか、２回押して通信遮断にするか、あるいは通話開始ボタンを押した後、あらかじめ決められた特定の数字を入力する、等のような「応答の際の本人識別のための特別の操作」をいう。
【００１３】また、情報処理センターのオペレーターと携帯電話機の所有者による音声による応答でも可能ではある。
【００１４】ここで、不正使用者により、その個人の識別情報が、本人が知らないうちに使われたような場合でも、その本人の携帯電話機の呼び出しがあるため、携帯電話機の所有者が通常の呼び出しと勘違いして不用意に操作して個人認証され（本人だと誤認され）、悪用されないよう、ここでの応答操作は、携帯電話機の通常の通話に使用する操作とは異なる特別の操作が好ましく、例えば、請求項８のように通話開始ボタンを押した後、暗証番号のような特定の数字を入力するのが、望ましい。この場合、暗証番号は各個人によりそれぞれ異なるため、応答操作すなわち入力された暗証番号の正否の判断のための照合用として、この暗証番号も個人の識別情報と共に記憶装置に登録しておく必要がある。
【００１５】このときに使用する暗証番号は、前記のように所有者本人が不用意に操作が出来ないという効果に加えて、他人の携帯電話機を所持している人に操作が出来ないようにする効果もある。なお、この個人認証方法に使用する携帯電話機は通常の携帯電話機を使用でき、携帯電話機に特別な付加機能などを設ける必要はない。
【００１６】この方法による個人認証方法がなぜ有効に機能するのかを述べると、通常の暗証番号による個人認証方法では、暗証番号が解読される可能性があるのに対して、この方法では、認定すべき個人を、その個人が所有する携帯電話機を呼び出して確認をとるため、仮に、万が一、不正使用者がその携帯電話番号を知っていたとしても、当該携帯電話機を所持していない第三者である

不正使用者は、その間の通信手段に割り込むことが不可能であるからである。また、先に述べたように、携帯電話機からの入力（応答操作）に暗証番号を使用する場合、他人の携帯電話機を所持していたとしても、暗証番号を知らない第三者には操作が出来ないので、携帯電話機の紛失、盗難に備えて、さらに安全性は高まる。

【００１７】ここで「携帯電話機」として表現しているが、移動通信手段であれば良く、したがってＰＨＳや通信機能を持ったＰＤＡ（個人用携帯情報端末）等も含まれるものとする。

【００１８】請求項３の個人認証システムは、以下の各手段で構成されている。

１．個人の識別情報（顧客番号、利用者名、住民番号など）および携帯電話番号が記録された個人カード（キャッシュカード、クレジットカード、メンバーズカード、行政ＩＣカード等）。

２．個人カードを使用して個人の識別情報および携帯電話番号を入力するための識別情報入力手段。

３．識別情報入力手段より入力された携帯電話番号の携帯電話機を呼び出す通信手段。

４．個人が所有（所持）する応答操作のための携帯電話機。

５．該携帯電話機より通信手段を介して送られた応答信号を正規な応答であるか判断する演算手段。以上の各手段を有するシステム構成により、演算手段の判断に基づき、その個人を本人であると認証する。

【００１９】請求項１の個人認証システムと異なる点は、携帯電話番号を記録しておく場所が情報処理センターや電子認証センターのコンピュータの記憶装置等の記憶手段ではなくて、個人カードそのものに記録しておく点である。したがって、この場合は、個人カードそのものが記憶手段として作用している。

【００２０】ここで、利用者本人による応答操作に、請求項８のように暗証番号が使われる場合、応答操作すなわち入力された暗証番号の正否の判断のための照合用として、この暗証番号も個人の識別情報や携帯電話番号と共に個人カードに記録しておく必要がある。

【００２１】この場合、第三者による個人カードの不正利用を防止するために、特に、携帯電話番号は容易に書き替えられないようにする必要がある。なぜなら個人カードが不正使用者である第三者の手に渡り、その第三者の携帯電話番号に書き替えられてしまえば、その人物が個人カードの正規の所有者だと誤認されるからである。

【００２２】このように、この場合は、カード内に携帯電話番号が予め記録されているため、情報処理センターや電子認証センターの記憶装置から携帯電話番号を検索する必要がなく、システムがより簡単に構築できる。

【００２３】請求項４の個人認証方法は、請求項３のシステムを用い、個人の識別情報（顧客番号）および携帯電話番号が記録された個人カード（例えばキャッシュカードやクレジットカード、メンバーズカード、行政ＩＣカードなど）を使用することにより、個人の識別情報および携帯電話番号が識別情報入力手段より入力されると、その個人の携帯電話番号の携帯電話機を、通信手段を介して呼び出し、該携帯電話機より特定の入力操作（応答操作）がなされたときは、その個人本人であると認定し、呼び出し後、ある一定時間内に正規の入力操作（応答操作）がなされないときは、否認することを特徴とする。

【００２４】請求項５の個人認証システムは、通信手段を介して互いに接続された複数のコンピュータ間において、運営者側のコンピュータが、利用者側のコンピュータの利用者個人を確認するための利用者の（個人）認証システムであり、以下のとおり構成される。

１．識別情報入力手段。

利用者は、利用者側コンピュータに、利用者（個人）の識別情報入力手段を持つ。ここで識別情報入力手段は、通常の入力キー（キーボード）を使用しても良いし、あるいは個人の識別情報をあらかじめハードディスクやフロッピー（登録商標）ディスクに登録しておいて、これを入力情報として使用しても良い。また、カードリーダーを使用することも出来る。

２．携帯電話機

利用者はさらに応答操作のための携帯電話機を持つ。

３．記憶手段

運営者側のコンピュータは、あらかじめ利用者の識別情報と、携帯電話番号を登録しておく記憶手段を持つ。

４．通信手段

運営者側（のコンピュータ）はさらに、利用者側コンピュータの識別情報入力手段より入力し送信された利用者（個人）の識別情報をもとに記憶手段より検索し読み出した携帯電話番号の携帯電話機を呼び出す通信手段を持つ。

５．演算手段

運営者側のコンピュータは、利用者の携帯電話機より通信手段を介して送られた応答信号を正規な応答であるか判断する演算手段を持つ。以上の構成により、前記の演算手段の判断に基づき、その個人を認証することを特徴とする個人認証システムである。

【００２５】請求項６の個人認証方法は、通信手段を介して互いに接続された複数のコンピュータ間において、利用者側のコンピュータの識別情報入力手段より利用者の識別情報が入力され送信されたとき、これを受信し、運営者側のコンピュータ（相手を利用者認定するべき側のコンピュータ）において、あらかじめ記憶手段に登録されたその利用者の携帯電話番号を、利用者（個人）の識別情報をもとに該記憶手段より検索して、その利用者の携帯電話機を通信手段を介して呼び出し、該携帯電話機より特定の入力操作がなされたとき、その信号を受信し適正な入力操作（応答操作）がなされたかを判断し、

その利用者本人であると認定することを特徴とする利用者の（個人）認証方法である。

【００２６】ここで、「利用者の個人認証方法」としているが、利用者は個人ばかりではなく、会社や学校等の団体にも適用できる。その場合は、必ずしも個人の携帯電話機である必要はなく、請求項７に記載のように、携帯電話機に代えて、通常の回線使用電話機でも実施可能である。

【００２７】この個人認証方法によると、インターネット等の広域ネットワーク、すなわち、通信手段を介して大規模ネットワークに接続された不特定多数のコンピュータ間において、相手の利用者認定をする場合に、さらにその効果を発揮できる。

【００２８】キャッシュカードやクレジットカード、メンバーズカードなどの各種個人カードを使用する場合と違って、インターネット上では、相手の人物や様子をうかがい知ることも出来ず、より利用者の認定が難しく、重要になってくるからである。

【００２９】ここで、利用者側のコンピュータと運営者側のコンピュータとは、常に固定的な立場ではなく、例えば、通常は利用者側のコンピュータとして使用している個人のパーソナルコンピュータを、他からの不正侵入に備えての接続許可の判断に、この利用者の個人認証方法を使用した場合、個人のパーソナルコンピュータが他の利用者を確認する運営者側のコンピュータとなりうる。

【００３０】したがって、この場合は、その個人のパーソナルコンピュータの記憶装置内に、接続を許可する通信相手の利用者の識別情報（顧客番号や顧客名など）と携帯電話番号を、あらかじめ登録しておく必要があり、また携帯電話機を呼び出す通信手段も持っておく必要がある。

【００３１】この個人認証方法は、例えば仕事先や出張先の携帯コンピュータから自宅のコンピュータに頻繁にアクセスして使用している人が、他の人には絶対にアクセス出来ないようにしたい場合などに有効である。

【００３２】請求項７について以上述べてきた利用者認定方法では、主に利用者個人の認定であることと、使用場所を限定出来ないキャッシュカード等の使用のために、携帯が可能であることを主眼において携帯電話機もしくはＰＨＳや通信機能を持ったＰＤＡ（個人用携帯情報端末）として表現しているが、例えばインターネットにて会社どうしで実施する場合等には、必ずしも携帯電話機である必要はない。

【００３３】したがって、パーソナルコンピュータの近傍に設置された、通常の回線使用電話機でも実施可能である。したがって、広義に解釈した場合は、請求項１から請求項６の個人認証システムおよび方法において、携帯電話機に代えて双方向通信機器を採用することができる。

【００３４】請求項８について請求項８は、請求項１から請求項７までに記載の個人認証システムおよび方法において、携帯電話機より入力される特定の入力操作（応答操作）として、暗証番号を用いるものである。携帯電話機からの入力に暗証番号を使用する場合、所有者本人が不用意に操作が出来ないという効果に加えて、暗証番号を知らない第三者に操作が出来ないので、携帯電話機の紛失、盗難に備えて、さらに安全性が高まる。この場合、暗証番号は各個人によりそれぞれ異なり、応答操作（すなわち暗証番号入力）の正否の判断のための照合用として、この暗証番号も個人の識別情報と共に記憶手段に登録しておく必要がある。

【００３５】ここで、観る視点を変えると、「あなたの暗証番号の入力は、あなたの携帯電話機から」ということになる。つまり、暗証番号は、本人確認のために呼び出された、その携帯電話機からしか受け付けない。したがって、第三者による不正使用は出来ないわけである。

【００３６】

【発明の実施の形態】次に本発明による個人認証システムおよび個人認証方法が実際上どのように具体化されるか実施形態を説明する。

実施形態１〔デビットカードシステムへの応用〕

まず、請求項１の個人認証システムを利用して請求項２の個人認証方法を実施する場合につき、図１、図３に基づいて説明する。図３において、Ｃはデビットカード（キャッシュカード）、Ｒはその読取りに使用するカードリーダー、１は金融機関等の情報処理センター、２は通信手段、３は携帯電話機である。

【００３７】ステップＳ１：デビットカードシステムの加盟店にてデビットカード（キャッシュカード）Ｃをカードリーダー Ｒに読み込ませ、読み取った顧客番号などの利用者識別情報を、金融機関等の情報処理センター１に送る。

【００３８】ステップＳ２：情報処理センター１では利用者識別情報をもとにコンピュータの利用者ファイルから、その利用者の携帯電話番号を検索する。

【００３９】ステップＳ３：その番号の携帯電話機３を呼び出す。

【００４０】ステップＳ４：当該携帯電話機３が呼び出されて、着信音が鳴ると、顧客は携帯電話機３より所定のキー操作すなわち応答操作をする。キー操作の例は、例えば次の通りである。

（イ）応答保留ボタンを一度押す→応答保留のアナウンス→（ロ）応答保留ボタンを二度押す→通信遮断。

（ハ）通信開始ボタンを押した後、暗証番号などの特定の数字を入力すると、数字に応じた信号が携帯電話機３より情報処理センター１へ発信される。

【００４１】ステップＳ５：応答信号を確認する。情報処理センター１では、通信手段２を介して送られてきた応答信号を正規の応答であるか判断する。ここで、呼び

出し音が一定の時間を超えて鳴るときは、応答なしとみなす。また応答操作に暗証番号を使用しているときは、暗証番号が登録時の暗証番号と一致しているかコンピュータにて照合して判断する。

【００４２】ステップＳ６：正規の応答ありの場合は、真正な顧客と認定し、デビットカードシステムの加盟店へ認定情報を送る。

【００４３】ステップＳ７：本システムによる個人認証が終了したので、他に必要な手続きへ進む。

【００４４】ステップＳ８：正規の応答がない場合、すなわち暗証番号が間違っていたり、ある一定時間内に応答がない場合は、真正な顧客とは認定されず、デビットカードシステムの加盟店へ否認情報を送る。

【００４５】ステップＳ９：そして否認後の、他に必要な手続きへ進む。

【００４６】以上の処理において、キャッシュカードやデビットカードの場合、現行のシステムを尊重する立場から、通常は従来の暗証番号のみで利用者を認定し、ある限度額を超えた高額の出金や決済の場合に携帯電話機の操作を要求してもよい。

【００４７】実施形態２〔住民が行政サービスなどを受ける際に必要となる本人確認への応用〕

【００４８】請求項１の個人認証システムを利用した請求項２の個人認証方法の実施形態２を、図１、図４に基づいて説明する。

【００４９】ステップＳ１：役所の窓口にて従来の印鑑に代えて住民Ａは個人カード（現在政府が策定中の行政ＩＣカード等）Ｃを提出し、これをカードリーダーＲ等の識別情報入力手段に読み込ませ、住民Ａの識別情報を電子認証センター１へ送信する。

【００５０】ステップＳ２：電子認証センター１では送信されてきた識別情報をもとにコンピュータの記憶装置より住民Ａの携帯電話番号を検索する。

【００５１】ステップＳ３：その番号の携帯電話機３を呼び出す。

【００５２】ステップＳ４：当該携帯電話機３が呼び出されて、住民Ａの携帯電話機３の着信音が鳴ると、住民Ａは携帯電話機３よりキー入力等による応答操作をし、その応答信号が電子認証センター１へ送信される。

【００５３】ステップＳ５：応答信号を確認する。電子認証センター１では通信手段２を介して送られてきた応答信号を正規の応答であるか判断する。ここで、呼び出し音が一定の時間を超えて鳴るときは、応答なしとみなす。また応答操作に暗証番号を使用しているときは、暗証番号が登録時の暗証番号と一致しているかコンピュータにて判断する。

【００５４】ステップＳ６：応答信号が正しければ認証成立とし、役所の窓口に設置されたディスプレイ５に認証成立の表示などを行なう。

【００５５】ステップＳ７：本システムによる個人認証が終了したので、他に必要な手続きへ進む。

【００５６】ステップＳ８：正規の応答がない場合、すなわち応答信号が間違っていたり、ある一定時間内に応答が何もない場合は、否認処理をする。例えば、役所の窓口に設置されたディスプレイ５に否認表示などを行なう。

【００５７】ステップＳ９：そして否認後の、他に必要な手続きへと進む。

【００５８】実施形態３〔防犯システムへの応用〕

【００５９】請求項３の個人認証システムを利用した請求項４の個人認証方法の実施形態３を、図２、図５に基づいて説明する。

【００６０】この実施形態は、重要な施設の出入口ドアなどに適する。

【００６１】ステップＳ１：施設の利用者は、従来の鍵の使用に代えて、各利用者の個人の識別情報および携帯電話番号が記録された個人カードＣをカードリーダーＲ等に読み込ませる。この個人カードＣは出入りを許可された者だけが持つ例えばメンバーズカードである。

【００６２】ここでは、実施形態１および２におけるステップＳ２に相当する手続きはなく、次のステップへそのまま続く。

【００６３】ステップＳ３：読み込んだ携帯電話番号の利用者の携帯電話機３をドアロックのコントローラー７より通信手段４を介して呼び出す。

【００６４】ステップＳ４：利用者が携帯電話機３より特定の入力操作すなわち応答操作をし、その応答信号がドアロックのコントローラー７へ送られる。

【００６５】ステップＳ５：通信手段４を介して送られた応答信号を正規の応答であるか、判断機能をもったドアロックのコントローラー７にて判断する。

【００６６】ステップＳ６：正規の応答があれば、その利用者本人であることを認定し、ドアロックを解除する。

【００６７】ステップＳ７：本システムによる個人認証が終了したので、他に必要な手続きへ進む。例えばステップ１に戻り、他の利用者のために個人カードの読み込み体制に戻す。

【００６８】ステップＳ８：正規の応答がない場合、すなわち応答操作が間違っていたり、ある一定時間内に応答が何もない場合、ドア６は開けられず、また例えば警告音を発する等の否認処理をする。

【００６９】ステップＳ９：そして、否認後の手続きへと進む。例えばステップ１に戻り、他の利用者のために個人カードの読み込み体制に戻す。

【００７０】ここで、利用者本人による応答操作に暗証番号が使われる場合、応答操作すなわち入力された暗証番号の正否の判断のための照合用として、この暗証番号も個人の識別情報や携帯電話番号と共に個人カードＣに記録しておく必要がある。

【００７１】実施形態４〔インターネット上での利用者認定方法への応用〕

【００７２】請求項５の個人認証システムを利用した請求項６の個人認証方法の実施形態４を、図１、図６に基づいて説明する。

【００７３】この実施形態は、インターネット等の広域ネットワークにおいて、相手の利用者認定を行ない接続許可の判断をする場合に適する。

【００７４】ステップＳ１：利用者側のコンピュータ８から利用者識別情報が入力され送信される。

【００７５】ステップＳ２：運営者側のコンピュータ９に於いてあらかじめ登録されたその利用者の携帯電話番号および暗証番号を、送信されてきた利用者識別情報をもとに記憶装置より検索する。

【００７６】ステップＳ３：次いで、その利用者の携帯電話番号を、通信手段２を介して呼び出す。

【００７７】ステップＳ４：携帯電話機３が呼び出されて、着信音が鳴ると、利用者は携帯電話機３の通話開始ボタンを押した後、暗証番号を入力し、その信号が運営者側のコンピュータ９へ送られる。

【００７８】ステップＳ５：運営者側のコンピュータ９は通信手段２を介して送信されてきた暗証番号が、記憶装置より読み出した暗証番号と一致するか判断する。

【００７９】ステップＳ６：暗証番号が正しければ認証成立とする。

【００８０】ステップＳ７：認証が成立したら、運営者側のコンピュータ９に接続する。

【００８１】ステップＳ８：正規の応答がない場合、すなわち暗証番号が間違っていたり、ある一定時間内に応答が何もない場合は、否認の判断が下される。

【００８２】ステップＳ９：運営者側のコンピュータ９への接続を拒否する。そして否認後の、他に必要な手続きへと進む。

【００８３】実施形態５〔パーソナルコンピュータを利用した電子決済システムへの応用〕

【００８４】請求項１、請求項５の個人認証システムおよび請求項２、請求項６の個人認証方法を応用した実施形態５を、図１、図７に基づいて説明する。

【００８５】この場合は、電子決済システムの利用契約をする金融機関もしくは情報処理センター１の記憶装置に、あらかじめ利用者識別情報および利用者の携帯電話番号および暗証番号を登録しておく。

【００８６】利用者に於いては、キャッシュカードに記録された利用者の識別情報および銀行口座情報を、使用しやすいようにあらかじめフロッピーディスク等の記録媒体もしくはハードディスク等の記憶装置内に登録しておく。あるいは、カードリーダーを直接パーソナルコンピュータにつないでキャッシュカードを使用することも出来る。

【００８７】この電子決済システムを利用する際は、次の手順で処理する。

【００８８】ステップＳ０：まず、パーソナルコンピュータ８を操作することにより、フロッピーディスク等の記録媒体もしくはハードディスク等の記憶装置もしくはカードリーダーから、利用者の識別情報および銀行口座情報を読み取り、取引情報（希望する取引の商品や決済の内容などの情報）と共に取引相手方のコンピュータ１０に送信する。このステップＳ０は、図１のフローチャートの入り口に相当する。

【００８９】ステップＳ１：電子決済システムの加盟店（者）である取引相手方のコンピュータ１０は、送信されて来た利用者識別情報（暗証番号も含む）、銀行口座情報（および取引情報）に、自身の加盟店（者）情報および取引金額を付加して、電子決済システムの金融機関もしくは情報処理センター１に送信する。

【００９０】ステップＳ２：金融機関もしくは情報処理センター１にて、あらかじめ登録されているその利用者の携帯電話番号を、利用者識別情報（顧客番号、利用者名など）をもとに記憶装置より検索する。

【００９１】ステップＳ３：その利用者の携帯電話機３を通信手段２を介して呼び出す。

【００９２】ステップＳ４：利用者の携帯電話機３の着信音が鳴り、利用者にとって当電子商取引を成立させてよいか確認のため、また、加盟店にとって必要な利用者の個人認証のため、利用者にキー入力による応答操作を促し、利用者は暗証番号を入力する。

【００９３】ステップＳ５：キー操作を確認する。すなわち、情報処理センター１では、携帯電話機３より送信されてきた暗証番号が、登録されている暗証番号と一致するか判断する。

【００９４】ステップＳ６：その利用者本人であると認定した場合は、利用者の銀行口座より加盟店（者）の銀行口座に取引金額を口座振り替えするとともに、加盟店（者）である取引相手方のコンピュータ１０へ認証成立および決済完了の情報を送信する。

【００９５】ステップＳ７：本システムによる個人認証および必要な手続きが終了したので、他に必要な手続きへ進む。

【００９６】ステップＳ８：正規の応答がない場合、すなわち暗証番号が間違っていたり、ある一定時間内に応答が何もない場合は、否認処理をし、取引相手方のコンピュータ１０へ否認の情報を送信する。

【００９７】ステップＳ９：そして否認後の、他に必要な手続きへと進む。

【００９８】

【発明の効果】以上のように、通常の暗証番号による本人確認方法や利用者認定方法では、暗証番号が解読される可能性があるのに対して、本発明の個人認証システムおよび個人認証方法によると、認定すべき個人を、その利用者が所有する携帯電話機を呼び出して確認をとるた

13

め、仮に、万が一、不正使用者がその携帯電話番号を知っていたとしても、第三者である不正使用者は、その間の通信手段に割り込むことが不可能となる。したがって、携帯電話機を所持している本人でなければ、携帯電話機のキーの操作ができないので、安全である。

【００９９】また、先に述べたように、携帯電話機からの入力時に、本人独特の暗証番号を使用する場合は、たとえ携帯電話機を窃盗して所持していたとしても、本人確認が不可能となるので、さらに安全性は高まる。

【図面の簡単な説明】

【図１】　請求項１、２、５、６および実施形態１、２、４、５を説明するフローチャートである。

【図２】　請求項３、４および実施形態３を説明するフローチャートである。

【図３】　実施形態１を説明する概念図である。

【図４】　実施形態２を説明する概念図である。

14

＊【図５】　実施形態３を説明する概念図である。

【図６】　実施形態４を説明する概念図である。

【図７】　実施形態５を説明する概念図である。

【符号の説明】

C　個人カード

R　カードリーダー

1　金融機関等の情報処理センター

2　無線通信手段

3　携帯電話機

4　有線通信手段

5　役所の窓口に設置されたディスプレイ

6　ドア

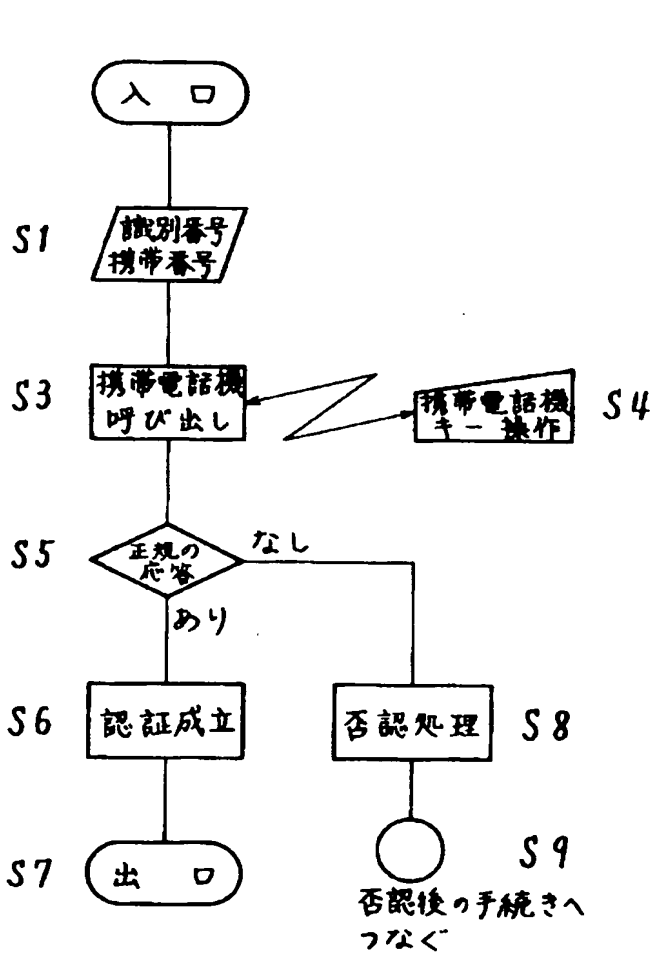
7　ドアロックのコントローラー

8　利用者側のコンピュータ

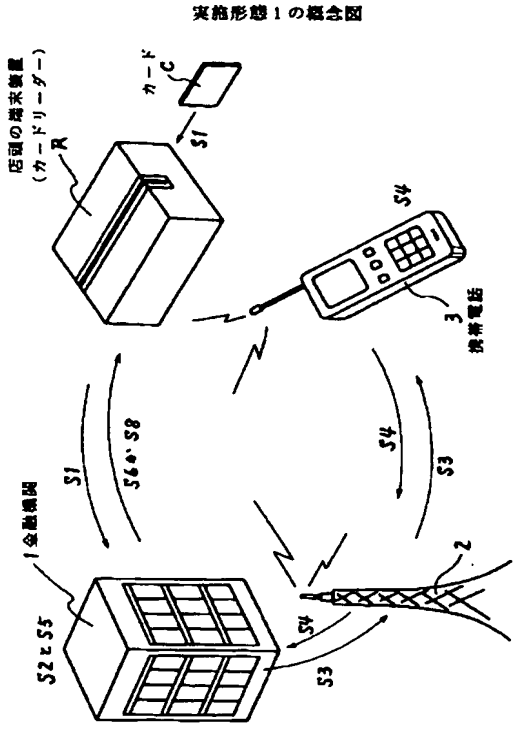
9　運営者側のコンピュータ

＊　１０　取引相手方のコンピュータ

【図２】

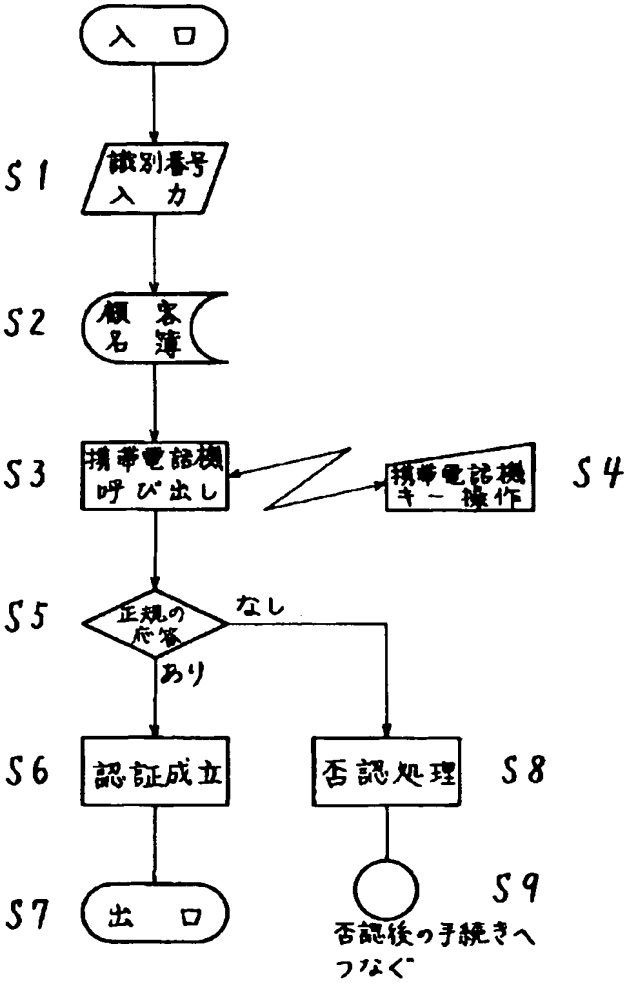


【図３】

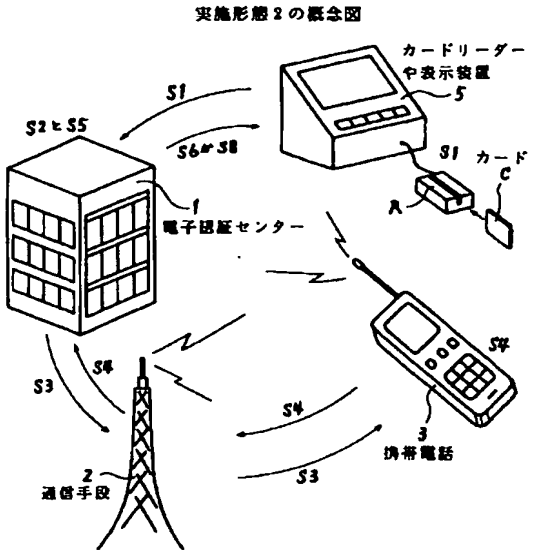


【図１】

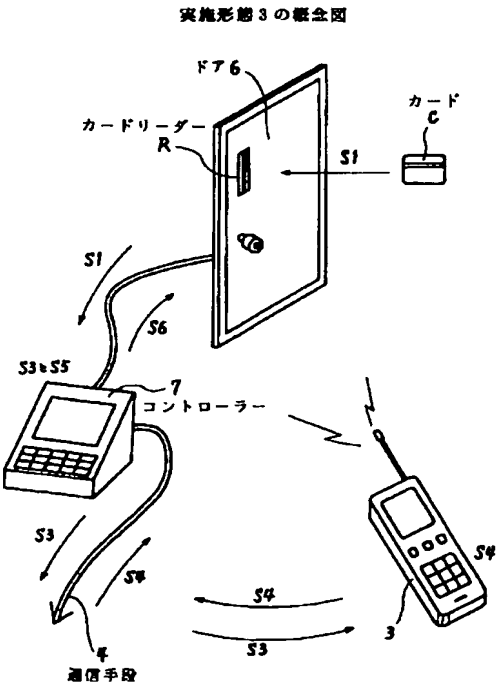
実施形態１、２、４、５の説明



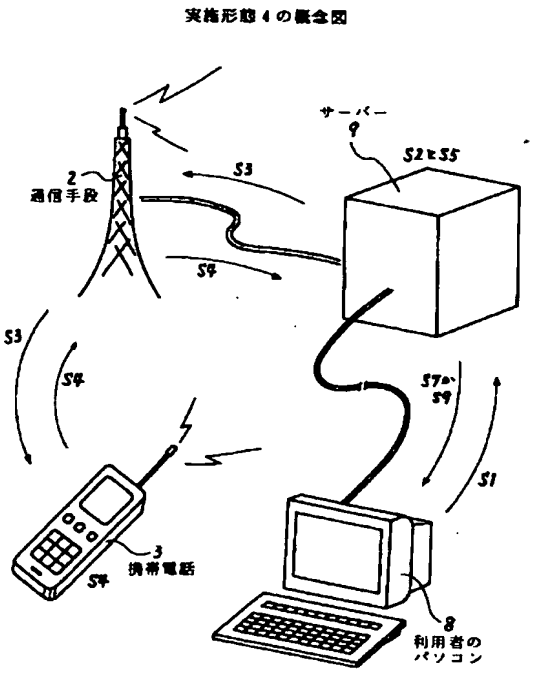
【図４】



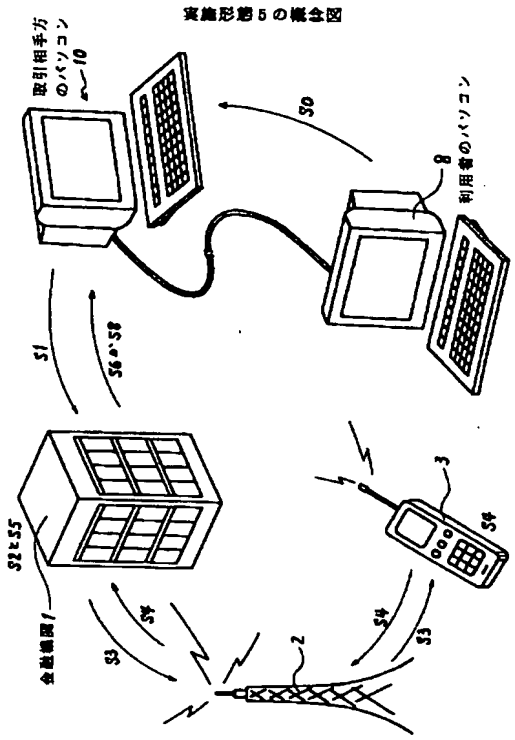
【図５】



【図６】


実施形態４の概念図
サーバー
9
S2とS5
2
通信手段
S3
S4
S3
S4
S7a
S9
S1
3
携帯電話
S4
8
利用者の
パソコン

【図７】


実施形態５の概念図
取引相手方
のパソコン
10
S0
8
利用者のパソコン
S1
S6・S8
S2とS5
3
S4
金融機関1
S3
S4
2
S4
S3